



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/604,944	06/27/2000	Marco A. DeMello	MSFT-0127/73297.3	5209
41505	7590	12/23/2004	EXAMINER	
WOODCOCK WASHBURN LLP			GURSHMAN, GRIGORY	
ONE LIBERTY PLACE - 46TH FLOOR			ART UNIT	
PHILADELPHIA, PA 19103			PAPER NUMBER	

2132

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/604,944

Applicant(s)

DEMELLO ET AL.

Examiner

Grigory Gurshman

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 October 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 7, 11, 14, 21, 22 and 24-64 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 7, 11, 14, 21, 22 and 24-64 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 10/22/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed on 10/22/2004 has been considered.

Response to Arguments

2. Applicant's amendment of the claims reflects including the limitations of the canceled claims into the remaining claims.
3. Referring to claims 7, 14, 22, 31, 32, 35, 36, 37, 47, 48, 49, 58, 59 and 60, Applicant argues that cited prior art does not teach the encryption of certain types of information recited in the instant claims. Examiner points out that all the types of encrypted information recited in the instant claims are explicitly taught by Levergood as stated in the rejection herein.
4. Referring to claims 21, 30, 39, and 63, Applicant argues that cited prior art does not teach the symmetric key recited in the instant claims. Examiner points out that Levergood teaches the use of a shared secret key. Levergood does explicitly teach sharing secret key between the authentication and content servers (see col. 5). While Levergood does not use the term "symmetric", one of ordinary skill in the art would have equated the shared secret key with the symmetric key. Applicant argues that Levergood does not provide any teachings that would make a secret key inherently a symmetric one as opposed to a secret asymmetric key. Examiner points out that Applicant's

arguments in this case are not well grounded. The "secret asymmetric key" is normally referred to as a private key in the asymmetric cryptography schema.

5. Referring to claim 24, Applicant argues that cited prior art does not teach the provision of two sets of software. Examiner respectfully disagrees and points out that the limitations of claim 24 are met as following:

- providing, to a first party for use on a first computing device, a first set of computer-executable instructions which encrypts information based on a unique id that maps into a shared secret, the encrypted information being includable in an HTTP request which includes a network address of a second computing device (col 5, line 54-65; first computing device is authentication server, second computing device is content server);
- providing, to a second party for use on said second computing device, a second set of computer-executable instructions which decrypts the encrypted information (col 6, line 21-26).

6. Referring to claims 33 and 44, Applicant argues that the instant claims have not been properly addressed. Examiner points out that the limitations of the instant claims are met as following:

Referring to claim 33, Levergood discloses a method of building a client-server request, said method comprising the acts of:

- encrypting first information so as to be decryptable by a secret accessible to a first server (col. 3, line 12-16; the first server is the content server);

- including an address associated with said first server in said client-server request (col. 3, line 12-16);

Referring to claim 44, Levergood discloses a method of distributing electronic content, said method comprising the acts of:

- receiving, at a first computing device (authentication server) from a second computing device (client browser), an order for a content item (col 8, line 61-63);
- providing, from said first: computing device to said second computing device, data comprising: a network address of a third computing device (content server); and encrypted information (SID); wherein said third computing device processes said order by using at least some of said encrypted information (col. 5, line 47-49).

7. Referring to claim 54, Applicant argues that the limitation "purchase transaction" is not inherent. Examiner respectfully disagrees and points out that in the art of downloading valuable content from the content servers, it is inherent to have purchase transactions.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 7, 11, 14, 21, 22, 24-27, 30-50, 52-54, 56-61, 63 and 64 are rejected under 35 U.S.C.102(b) as being anticipated by Levergood et al. (US Patent 5,708,780; "Levergood" hereinafter).

Referring to the independent claim 7, Levergood discloses a method of communicating with a first computing device comprising:

- encrypting information (SID) destined for said first computing device (col 5, line 54-60; content server is the first computing device);
- creating an HTTP request which includes an address of said first device and the encrypted information (col. 6, line 20-22 [http://content.com/\[SID\]/report](http://content.com/[SID]/report));
- transmitting a web page comprising the HTTP request to a second computing device different from said first computing device (col. 6, line 23-24; client browser represents the second computing device, content server represents the first computing device).

10. Referring to claim 7, Levergood also discloses the second computing device associated with a purchaser of content (col. 8, line 61-62), wherein said first computing device provides said content (col. 5, line 40-41), and wherein the encrypted information includes information relating to the purchase of said content (col 5, line 54-60).

Levergood teaches that encrypted information includes information, which identifies said purchaser (col 5, line 60 user identifier).

11. Referring to claim 11, Levergood discloses a computer readable medium having computer-executable instructions to perform the method of claim 1 (col 4, line 24-28).

12. Referring to the independent claim 14, Levergood discloses a method of communicating with a first computing device through a second computing device, the method comprising the acts of:

- encrypting information such that the encrypted information is decryptable by a secret (col. 6, line 8; SID);
- transmitting the encrypted information to said second computing device, said encrypted information being transmittable to said first computing device upon instruction from a user operating said second computing device, wherein said secret is not accessible to either said second computing device or said user (col. 3, line 11-20; first computing device is content server, second computing device is client browser);
- sharing said secret by performing either of the following acts: providing said secret to said first computing device or to a party associated with said first computing device; or receiving said secret from said first computing device or from a party associated with said first computing device (col. 5, line 64-65).

13. Referring to the independent claim 21, Levergood discloses a method of communicating with a first computing device through a second computing device, comprising the steps of:

- encrypting information such that the encrypted information is decryptable by a secret (col. 6, line 8; SID);
- transmitting the encrypted information to said second computing device, said encrypted information being transmittable to said first computing device upon instruction

from a user operating said second computing device, wherein said secret is not accessible to either said second computing device or said user (col 3, line 11-20; first computing device is content server, second computing device is client browser);

- sharing said secret by performing either of the following acts: providing said secret to said first computing device or to a party associated with said first computing device; or receiving said secret from said first computing device or from a party associated with said first computing device (col. 5, line 64-65).

14. Referring to claim 21, Levergood teaches encrypting the information with the symmetric key (col. 5, line 64 secret key).

15. Referring to claim 22, Levergood discloses including a timestamp in the encrypted information (col. 3, line 34).

16. Referring to claim 24, Levergood discloses a method of facilitating electronic content distribution comprising the acts of:

- providing, to a first party for use on a first computing device, a first set of computer-executable instructions which encrypts information based on a unique id that maps into a shared secret, the encrypted information being includable in an HTTP request which includes a network address of a second computing device (col 5, line 54-65; first computing device is authentication server, second computing device is content server);

- providing, to a second party for use on said second computing device, a second set of computer-executable instructions which decrypts the encrypted information (col 6, line 21-26).

17. Referring to claim 25, Levergood teaches the first party comprising a seller of electronic content (col. 8, line 61-62; the user may purchase the subscription to gain access to document), wherein the second party comprises a provider of electronic content sold by said first party (content server provides information), and wherein the encrypted information relates to a transaction between the first party and a consumer of electronic content (SID).

18. Referring to claim 26, Levergood teaches that HTTP request comprises a POST request, and wherein said encrypted information is included in the body of said POST request (col. 7, line 7-11).

19. Referring to claim 27, Levergood teaches that HTTP request comprises a GET request, and wherein said encrypted information is appended to said GET request as a parameter (col. 5, line 32-33; col. 5, line 53-54).

20. Referring to claim 30, Levergood teaches a secret symmetric key to encrypt the information (col. 5, line 64).

21. Referring to claim 31, Levergood teaches that the information includes information identifying an item of content, which said second computing device provides (col 3, line 59-60).

22 Referring to claim 32, Levergood teaches that the information includes information identifying a purchaser of an item of content (col. 5, line 60).

23. Referring to claim 33, Levergood discloses a method of building a client-server request, said method comprising the acts of:

- encrypting first information so as to be decryptable by a secret accessible to a first server (col. 3, line 12-16; the first server is the content server);
- including an address associated with said first server in said client-server request (col. 3, line 12-16);
- including the encrypted information in said client-server request (col. 3, line 12-16; col. 7, line 21-34).

24. Referring to claim 34, Levergood discloses wherein the encrypted information includes information relating to a transaction to purchase a content item, wherein said first server furthers at least some aspect of said transaction (col. 8, line 31-33).

25. Referring to claim 35, Levergood teaches that encrypted information includes information which identifies a purchaser of the content item (col. 8, line 2).

26. Referring to claim 36, Levergood teaches that the encrypted information includes information, which identifies the content item (col. 8, line 3).

27. Referring to claim 37, Levergood teaches that encrypted information includes a timestamp (col. 8, line 3).

28. Referring to claim 38, Levergood teaches that the first server provides the content item (col. 8, line 11-13; Fig 3, Item10).

29. Referring to claim 39, Levergood teaches that encrypted information is generated by encrypting cleartext information with the symmetric key (col. 5, line 64).

30. Referring to claim 40, Levergood discloses client-server request comprises an HTTP request (col. 7, line 24-34).

31. Referring to claim 41, Levergood discloses wherein said HTTP request comprises a POST request, and wherein the encrypted information is included in the body of said POST request (col. 7, line 25-27).

Referring to claim 42, Levergood discloses wherein said HTTP request comprises a GET request, and wherein the encrypted information is appended to said GET request as a parameter (col. 7, line 29-34).

32. Referring to claim 43, Levergood discloses a computer-readable medium having computer-executable instructions to perform the method of claim 33 (col 4, line 26).

33. Referring to claim 44, Levergood discloses a method of distributing electronic content, said method comprising the acts of:

- receiving, at a first computing device (authentication server) from a second computing device (client browser), an order for a content item (col 8, line 61-63);
- providing, from said first: computing device to said second computing device, data comprising: a network address of a third computing device (content server); and encrypted information (SID); wherein said third computing device processes said order by using at least some of said encrypted information (col. 5, line 47-49).

34. Regarding claim 45, Levergood teaches that data comprises an HTTP POST request, and wherein the encrypted information is included in the body of said POST request (col. 7, line 7-11).

Regarding claim 46, Levergood teaches that data comprises an HTTP GET request (col. 5, line 32-33; col. 5, line 53-54).

Regarding claim 47, Levergood teaches that data encrypted information includes information identifying said content item (col. 5, line 54-61).

35. Regarding claim 48, Levergood teaches that data encrypted information includes information identifying the individual who issued said order for said content item (col. 5, line 59-60).

36. Regarding claim 49, Levergood teaches that encrypted information includes a timestamp (col. 5, line 57).

Regarding claim 50, Levergood teaches that data further comprises a hash of the encrypted information, the hash being computed prior to encryption of said information (col 5, line 62).

37. Regarding claim 52, Levergood teaches that content item does not reside on the first computing device (col. 5, line 59).

38. Regarding claim 53, Levergood teaches a computer-readable medium having computer-executable instructions to perform the method of claim 44 (col. 4, line 24-28).

39. Regarding claim 54, Levergood discloses a computer-readable medium having computer-executable instructions for performing steps comprising:

- receiving parameters that identify characteristics of a first transaction between a first client and a first server (col. 5, line 49, the parameter is SID, first client is client browser, first server is authentication server);
- encrypting one or more of said parameters (col. 5, line 64, encrypted with a secret key which is shared by the authentication and content servers);
- returning said encrypted parameters to said first client in a format such that a second server may receive said encrypted parameters from said first client (col 3, line 16-20), validate said first transaction, and initiate a second transaction without any interaction with said first server (Fig 2A, Item 100 Get URL through Item 106, second server is content server).

40. Regarding claim 56, Levergood teaches that the first transaction relates to the sale of electronic content (col. 8, line 62).

41. Regarding claim 57, Levergood teaches that the second transaction comprises downloading the electronic content from the second server to the first client (Fig 2A, Item Browser/Display).

42. Regarding claim 58, Levergood teaches that parameters comprise end-use information that enables the individualization of the electronic content (col. 5, line 59, a set of information file).

43. Regarding claim 59, Levergood teaches that parameters include one or more of the following: information identifying a party to the first transaction, and information identifying an item purchased in the first transaction (col. 5, line 54-61, user identifier).

44. Regarding claim 60, Levergood teaches containing a timestamp in encrypted parameter (col. 5, line 57)

45. Regarding claim 61, Levergood discloses computing a hash of at least some of the encrypted parameters (col. 5, line 62, hash).

Regarding claim 63, Levergood teaches that encrypting act comprises applying a secret symmetric key shared between the first server and the second server (col. 5, line 64-65)

46. Regarding claim 64, Levergood teaches that format comprises an HTTP request including an address of the first server (col. 5, line 54 [http://content.com/\[SID\]/report](http://content.com/[SID]/report)).

Claim Rejections - 35 USC § 103

47. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

48. Claims 28-29, 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US Patent 5,708,780, "Levergood" hereinafter) in view of Barnes et al. (US Patent 5,970,475, "Barnes" hereinafter).

49. Regarding claims 28-29, 55, Levergood discloses computer-executable instructions which encrypts information. Levergood fails to teach using COM object to perform the job. Barnes teaches the EC system core functionality is implemented using many Microsoft's component object model (COM) for the purpose of providing a specific function role and providing a function interface that can be accessed by other COM objects or COM-enabled processes (col 10, line 51-56). It would have been obvious to a person of ordinary skill in the art at the time of the applicant's invention was made to implement computer-executable instructions as COM object for providing a specific function role and providing a function interface that can be accessed by other COM objects or COM-enabled processes (see Barnes col. 10, line 51-56).

50. Claims 51 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US Patent No. 5,708,780) in view of Eberhard et al. (US Pub. 200110011238 A1).


51. Regarding claims 51 and 62, Levergood discloses hashing the encrypted information. Levergood fails to teach hashing the encrypted information using an SHA1 algorithm. Eberhard teaches hashing parameters by using a SHA1 algorithm to calculate a hash for a title file downloaded from the publisher's server for the purpose of maintaining integrity, doing comparison before the purchased title being downloaded (page 4, block 40-42). It would have been obvious to a person of ordinary skill in the art at the time of the applicant's invention was made to use SHA1 algorithm to maintain data integrity.

Conclusion

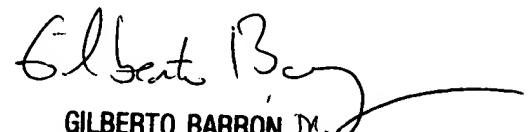
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


GG

Grigory Gurshman
Examiner
Art Unit 2132


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100